B9

(54) **Password-protected data link**

(57) A password-protected data communication system for transfer of data between remote user terminals and a host computer via public telephone lines and the like is further made secure by virtue of the fact that password transactions and/or interchanges are automatically effected between special modems provided at the user terminals and at the host computer without action or intervention (other than call initiating action) by the users who are denied access to or control over the passwords. A callback facility may also be provided and can be structured to enable users to communicate with the host from non-static locations.

GB 2 168 831 A

SPECIFICATION

Improvements relating to computer systems

5 This invention concerns improvements relating to
computer systems and more particularly concerns
the protection of host computers from unauthor-
ised access via remote terminals coupled with the
host computer over public communications net-
10 works including the public telephone system.
    As is well known, it is customary to provide a
user wishing to access a host computer, for exam-
ple a database to be interrogated or searched by
the user, with a unique user identification or pass-
15 word and to provide at the host computer a table
of user identifications for which access to the com-
puter database is permitted. The user's terminal is
customarily connected via a modem to the public
telephone network, for example, which in turn con-
20 nects via a corresponding modem with the host
computer. The user, when wishing to access the
host computer, calls the telephone number of the
host computer, receives an answering tone when
the telephone line connection is established, and
25 then enters his user identification via his terminal
keyboard; the user identification must be received
and verified at the host computer in order for ac-
cess to be provided.
    Whilst the provision of user identification pass-
30 words to be verified at the host computer before
access is permitted does provide e baseline level
of security against unauthorised eccess, nonethe-
less it does not in many situations provide for suf-
ficient security. Computer systems which can be
35 reeched through the public telephone system are
potentially vulnerable to unauthorised acces by
enyone who has by whatever meens improperly
come into possession of an authorised user identi-
fication password and further sophisticated com-
40 puter based techniques exist whereby
unauthroised entry can be obtained once the dial-
up telephone number of a computer facility has
been obtained.
    To further protect against such fraudulent ac-
45 cess, efforts have been made to implement less
readily determinable user passwords, end also au-
tomatic disconnection of the incoming terminal
line has been utilised following a small number of
invalid attempts to enter an acceptable password.
50 A more recent proposal has been to provide a so-
called port protection device external to the host
computer's dial-up access ports, the port protec-
tion device having on-board microprocessor intelli-
gence which is used to provide a level of external
55 password protection to any communication line.
The port protection device requires a potential dial-
up terminal user to manually enter a password as
a first step towards connecting with the host com-
puter, and the device then compares this password
60 with a table of valid user passwords stored in its
own memory. If the user-entered password
matches a previously stored password in the port
protection device memory is the user enabled to
proceed with the routine logging-on procedure at
65 the host computer involving entry of a further

password etc.
    As yet a further proposal, it has also been sug-
gested to introduce a callback facility into a port
protection device; since most legitimate users of a
70 host computer system can be presumed to have a
routine work station at a fixed location, the ration-
ale behind the callback proposal is that the port
protection device would instruct a user to hang-up
once his password had been verified and then
75 would call up a telephone number called from its
own memory and associated in the memory with
the password entered by the user; by this means
only a user in possession of a proper password
and located at the work stetion customarily associ-
80 ated with that password would be able to access
the host computer.
    According to the principal aspect of the present
invention, it is proposed that the modems provided
at each end of the data communication line, that is
85 at the user's terminal end and at the host com-
puter end, automatically carry out the password
transaction(s) or interchange(s) without action or
intervention by the user who, in accordance with
the invention, is denied access to or control over
90 the password(s). By this means, a very long and
potentially indeterminable password comprising
virtually en infinite number of possible character
combinations (that is to say a virtually infinite
"keyspece" size) can be utilised; by eutometic use
95 of such e comprehensive password, which has
meny meny more digits then could possibly be re-
membered and manuelly entered et a terminal,
and by not revealing the password to the terminal
end user much greater security of access is in-
100 sured.
    In a practical situation therefore, the conven-
tional modems which would customarily be pro-
vided at each end of the communication line would
be replaced by special modems configured, in ac-
105 cordance with the invention, to include means for
exchanging the necessary password(s), and means
to enable password(s) to be entered during manu-
facture of the modem and, if desired, to the cus-
tomer's specification, such meens including, for
110 example, provision in the modem of appropriately
programmed memory media. Autodial facilities
would also be associated with each of the modems
or at least with the user end modem.
    In operation of a system in accordance with the
115 invention, the user will by appropriate operation of
his terminal cause his modem to initiate a call to
the host's modem, which requires the user's mo-
dem to transmit its preprogrammed password. On
receipt of e valid password verified by comparison
120 with a password store at the host modem, the
host's modem euthorises direct connection of the
user to the host system. Should the host's modem
feil to receive a valid password, connection to the
host system will be prohibited. The rationale un-
125 derlying the invention is thus that the terminal user
need have no knowledge of the password(s), nor
even of the host computer's telephone number if,
for exemple, the terminal/host is a dedicated sys-
tem, and thus a principel source for fraudulent ac-
130 cess is elimineted.

The user's end modem may also be used in a conventional data communications link, i.e. to a non-protected system.

The system according to the invention can also incorporate a callback facility as aforesaid so as to further enhance the level of security provided by the system. With hitherto disclosed port protection devices incorporating a callback facility, entry of the passwords is (to our knowledge) by manual means; the present invention provides the facility for automatic transmission of the password by the user and modem. Further features which can be provided in a system in accordance with the present invention comprise the association of a status code and/or a time-of-access zone with each valid password. The status code can provide for immediate access of a special status authorised caller to the host computer thus bypassing the need for callback to be effected, end the time-of-access zone may be used to prevent an authorised user's access to the host computer at times other than those defined by his allocated time-of-access zone.

In accordance with yet a further aspect of the present invention, in order to enable a callback system to be utilised from any workstation location and to be utilised by users, such as travelling sales-persons for example, having mobile workstations with no fixed location and a variable telephone number, it is proposed that the host modem or port protection device, in response to verification of a received password transmitted by a user to-gether with the user's current telephone number location, generates a one-time short-term pass-word and transmits it back to the user's location. The user then has to re-dial the host computer and can obtain access only by use of the one-time short-term password within a predetermined short time period of the original password entry. The re-dialling of the host computer could be effected by means of autodial equipment provided in the mo-dem at the user's terminal end, the user's end mo-dem receiving and temporarily holding the one-time password transmitted by the host's modem; by this means the need for user knowledge or con-trol of passwords is completely removed thereby enhancing security.

In the systems according to the invention, the passwords, the user status codes and time-of-ac-cess zones, and the callback telephone numbers, or any of them, are not made accessible for modifica-tion by the standard user; that is to say, such data can be modified only at the command of an appro-priately authorised key person at the host com-puter location with such key person's access to the host computer itself being password controlled.

Having thus described the concepts upon which the present invention is based and recognising the capability of the skilled technician in the data com-munications art readily to put the herein-disclosed inventive concepts into practical realisation without need for further explanation, it is considered that no further description of the present invention is required herein. Various features, alterations and modifications will occur to those possessed of ap-propriate skills without departure from the spirit and scope of the invention. Basically the invention provides for security procedures to be completely hidden from the user and involves no user inter-vention.

As yet a further feature, the invention could make use of encryption techniques for yet higher levels of security.

CLAIMS

1. A password-protected data communication system for transfer of data between remote user terminals and a host computer via public tele-phone networks or the like and wherein password transaction(s) and/or interchange(s) are automati-cally effected between special modems provided at the user terminal and at the host computer without action or intervention (other than call initiating ac-tion) by the user who is denied access to or control over the password(s).

2. A system in accordance with claim 1 includ-ing a callback facility whereby, in response to re-ception at the host modem of an acceptable password, the host modem automatically seeks to connect the host computer with a predetermined user workstation location associated with the re-ceived password.

3. A system in accordance with claim 2 wherein the host modem, in response to verification of a received password transmitted by a user together with the user's current telephone number, gener-ates a one-off short-term password and transmits it back to the user's location, the user being enabled to access the host computer only by utilisation of such one-off short-term password within a prede-termined limited time period.

4. A system in accordance with claim 3 wherein the modem at the user's location is adapted and arranged to automatically access the host com-puter by utilisation of said one-off short-term pass-word without intervention from the user.

5. A system in accordance with any of the pre-ceding claims wherein the passwords utilised by the system incorporate user status and/or time-of-access zone codes.